Submission for *Designs, Codes and Cryptography*

Quantum Conference Key Distribution Systems

Key Words

Quantum cryptography

Conference key distribution

Information theory

Correlation

Quantum Conference Key Distribution Systems

Yi Mu and Yuliang Zheng

Center for Computer Security Research, Department of Computer Science,
University of Wollongong, Wollongong, NSW 2522, AUSTRALIA
Email: {yi, yuliang}@cs.uow.edu.au

and

Yan-Xia Lin

Department of Applied Statistics,
University of Wollongong, Wollongong, NSW 2522, AUSTRALIA
Email: yanxia@uow.edu.au

Abstract

We develop cryptographic protocols for conference key distribution systems based on the uncertainty principle in quantum physics. The information theoretical limits to the system correlation between users are demonstrated to describe quantum-cryptographically protected multi-user optical communication channels. An estimation of eveasdropping via "intercept/resend" for each quantum system is given. It is shown that such attacks can be revealed from the information and correlation formalism.

Key wards: Quantum cryptography, Conference key distribution, Information, Correlation.

1 Introduction

Quantum cryptography, a combination of quantum physics and cryptography, employs quantum mechanical phenomenon such as Heisenberg's uncertainty principle [1] [2] and quantum correlation - Einstein-Podolsky-Rosen-Bohm *gedankenexperiment*(EPR)[3] [4] to protect distributions of crytopraphic key. For the former scheme, information is enclosed on one of pair of non-commuting observable so that any attempt to extract the information by measurement of a eavesdropper will destroy some information. This causes a change in the signal between the legitimate users, which therefore reveals the the presence of the eavesdropper. For the later technique, the secure quantum key distribution can also be achieved by exploitation of the properties of quantum-correlated particles. In this scheme, any eavesdropping unavoidably adds some local condition which causes the measured data by legitimate users will display no violation of Bell's inequality and then revealing the attempt at interception. The technique without using Bell's inequality has been also developed by Bennett *et al*[5].

A recent experiment [2] has demonstrated a protocol of quantum key distribution which can in principle prevent any eavesdropping attacks including intercept/resend and beamsplitting. However in order to overcome a beamsplitting attack which uses only a small amount of signal beam without being detected any intensity losses, very dim light pulses had to be used. This therefore limits the transmission distance to about 32 cm. It is noted that an experimental work has demonstrated a single-photon transmission being up to 10 km by using single photon interference technique, a time-division Mach-Zehnder interferometer [6], which could be a good approach for quantum cryptographic systems. In a realistic telecommunication system, a long haul information transmission is achieved by high power light signal to overcome losses in optical fiber. Therefore, we have recently developed a higher power quantum cryptographic system, using state-mixing technique, which has been proved secure against any attacks including beamsplitting [7].

The progress in the theory and experiment of quantum cryptography for two-user systems has be made rapidly, therefore to study quantum cryptography for multi-user systems becomes interesting. Multi-user key distribution is called conference key distribution. A classical conference key protocol was studied by Ingemarsson *et al*[8]. However, a quantum channel is different in that it is a closed-single-line channel and so only does communication between two users be allowable, while a classical channel can be allowed to extract information by multiusers. In this paper, we study conference key distribution

protocols based on BB protocol [9][1][2]. The system information theory and correlation between users are studied for two basic conference key distribution systems: fun-shaped and series configuration.

The rest of this paper is organized as follows. Section 2 introduces our conference key distribution models. Section 3 is devoted to studying information theory on the conference key distribution protocols. Section 4 presents the theory of correlation function. In the final section, we discuss some the conference key distribution systems which consist of some basic conference key protocols studied in previous sections and summarize our work.

2 Conference Key Distribution Protocols

The quantum cryptographic communication based on BB protocol involves two users, say Alice and Bob, who share no secret information, together with an adversary Eve who eavesdrops on their communications. Under BB protocol, there are orthogonal and closed bases $B_1 = \{|\rightarrow\rangle, |\leftarrow\rangle\}$ and $B_2 = \{|\uparrow\rangle, |\downarrow\rangle\}$ related to different polarization. In order to measure these states, we introduce two quantum-mechanical operators, $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$, which have eigenstates in bases B_1 and B_2, respectively. The corresponding eigenequations then are

$$\hat{O}_{B_1}|\rightarrow\rangle = \mu_0|\rightarrow\rangle, \quad \hat{O}_{B_1}|\leftarrow\rangle = \mu_1|\leftarrow\rangle, \tag{1}$$

$$\hat{O}_{B_2}|\uparrow\rangle = \nu_0|\uparrow\rangle, \quad \hat{O}_{B_2}|\downarrow\rangle = \nu_1|\downarrow\rangle, \tag{2}$$

where eigenvalue μ_0 or ν_0 denotes binary code "0" and eigenvalue μ_1 or ν_1 denotes binary code "1". $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$ do not commute, i.e. $[\hat{O}_{B_1}, \hat{O}_{B_2}] \neq 0$ that results in Hesienberg's uncertainty principle, which suggests that a measurement on any state using a wrong basis will randomize the state. In BB protocol Alice sends a random sequence of all four canonical kinds of polarized photons to Bob. Bob randomly and independently chooses one of measuring bases to measure each photon pulse. They discuss publicly the bases Bob has used and discard those which disagree and keep secret on the identity of photon polarization. The remaining photon pulses can then be used in secret key distribution.

A multi-user cryptosystem involves complicated cryptographic communication, including quantum key distributions and system configurations, since a quantum cryptographic channel is based on two-user communication. In Fig. 1 (a) and (b), we introduce two quantum conference key distribution systems for N legitimate users $U_0, U_1, U_2, ..., U_{N-1}$.

Fig. 1 (a) presents a fun-shaped configuration; and (b) presents a series configuration. Many other configurations can be constructed in terms of these.

In the case of fun-shaped configuration, we consider two ways for the key propagation between legitimate users. For method one or type F_1, we consider a quantum protocol similar to BB protocol, where as a main user or a chair, U_0 sends a random sequence of single-photon pulses based on either B_1 or B_2 (with a 50/50 of chance) to $U_1, U_2, U_3, ..., U_N$ respectively. All beams should be identical. Subsequently, receivers measure each photon pulse using the measuring bases, B_1 or B_2 randomly and independently. Different from the BB protocol of two-user situation, in the public discussion U_0 has to be told which basis has been chosen for each photon pulse by all other users, then she tells them which measuring basis is correct. The correct basis represents the basis all users correctly used in the relevant measurement. They then agree to discard the measurement which is incorrect. The remaining photon pulses, which have been correctly measured, are used as a shared key distribution in future secure communications.

In above case, if a photon state (sent to all other users by U_0), say $|\alpha\rangle_{U_0}$, survives in all measurement via legitimate users, it is used for the key distribution. We assume that there is a common operator $\hat{U}$ responsible for the measurement of $|\alpha\rangle_{U_0}$, where $|\alpha\rangle_{U_0}$ is an eigenvector of $\hat{U}$. Then all elements in the final key distribution are obtained in terms of the measurement:

$$\hat{U}|\alpha\rangle_{U_0} = \alpha|\alpha\rangle_{U_0}, \tag{3}$$

where $\alpha \in \{\text{“0”}, \text{“1”}\}$, $|\alpha\rangle_{U_0} \in \{|\rightarrow\rangle, |\leftarrow\rangle, |\uparrow\rangle, |\downarrow\rangle\}$, and $\hat{U} \in \{\hat{O}_{B_1}, \hat{O}_{B_2}\}$. More explicitly,

$$\hat{U} = \begin{cases} \hat{O}_{B_1}, & \text{when } \hat{U}_0 = \hat{U}_1 = ...\hat{U}_{N-1} = \hat{O}_{B_1}, \\ \hat{O}_{B_2}, & \text{when } \hat{U}_0 = \hat{U}_1 = ...\hat{U}_{N-1} = \hat{O}_{B_2}. \end{cases} \tag{4}$$

$\hat{U}_i$ is obtained by choosing $\hat{O}_{B_1}$ and $\hat{O}_{B_2}$ randomly and independently,

$$\hat{U}_i = \text{Rand}(\hat{O}_{B_1}, \hat{O}_{B_2}), \qquad (i = 0, 1, 2, ..., N-1), \tag{5}$$

where Rand is either $\hat{O}_{B_1}$ or $\hat{O}_{B_2}$ in terms of a random number generator. It is easy to find that the probability for a single-photon pulse to survive from the measurements is $2^{-(N-1)}$, which suggests that the probability is a decreasing function of the number of user.

For method two or type F_2 (also Fig. 1(a)), a conference key distribution is established by utilizing a combined channel. As a chair, U_0 first generates a conference key distribution

herself using her own random number generator. In order to send the conference key distribution to other legitimate users, she has to establish private keys with all other users through quantum channels, so based on BB protocol the communications for private quantum key establishment are initially carried out "in pair", $U_0 \leftrightarrow U_1$, $U_0 \leftrightarrow U_2$, $U_0 \leftrightarrow U_3$, ... Then the private quantum key distributions are obtained. We denote them as $k_{U_0U_1}$, $k_{U_0U_2}$, $k_{U_0U_3}$... Obviously, U_0 knows all information of the key distributions. In order to send the conference key distribution, say K_{conf}, to another user, say U_i, K_{conf} chosen previously must have the same size as that of the local private key distribution $k_{U_0U_i}$ of U_0 and U_i. After all private keys have been established, the conference key can be sent to all legitimate users through a *classical* channel. The information sent to U_i through the classical channel is a Boolean addition between these keys,

$$C_{0i} = K_{conf} \oplus k_{U_0U_i}, \tag{6}$$

which releases no information to an eavesdropper. The conference key can be extracted by U_i in terms of

$$K_{conf} = C_{0i} \oplus k_{U_0U_i}. \tag{7}$$

For the series configuration, Fig. 1 (b), we also consider two ways to establish a conference key distribution. The first or type S_1, similar to type F_1, U_0 the main character or chair sends a random sequence of information to U_1 in terms of BB protocol; after measuring each photon pulse following Bob's way U_1 then reproduces and sends those that have been correctly measured to U_2; U_2 follows the same approach to pass the information, which survives, to U_3; one after the other until the final user receive the information. U_0 of course knows all information, since from users' public discussion she knows which photon pulse has survived after final user's measurement, and so is able to determine which pulse will be used to the conference key distribution that will be shared by all legitimate users. The discussion on Eq. (3) is also suitable for this system.

For the second case of series configuration, type S_2, similar to type F_2, U_0 generates a conference key distribution, then private-key establishment should start between all pairs, $U_0 \leftrightarrow U_1$, $U_1 \leftrightarrow U_2$, $U_2 \leftrightarrow U_3$, ..., based on BB protocol. The conference key distribution chosen by the chair is sequentially propagated from U_0 to other legitimate users one after the other via Boolean addition through a classical channel. Each user plays a role as a repeater,

$$U_0 \rightarrow U_1 : \quad C_{01} = K_{conf} \oplus k_{U_0U_1}, \quad K_{conf} = C_{01} \oplus k_{U_0U_1};$$

$$U_1 \to U_2: \quad C_{12} = K_{conf} \oplus k_{U_1U_2}, \quad K_{conf} = C_{12} \oplus k_{U_1U_2};$$
$$U_2 \to U_3: \quad C_{23} = K_{conf} \oplus k_{U_2U_3}, \quad K_{conf} = C_{23} \oplus k_{U_2U_3};$$
$$\ldots\ldots$$

Eavesdropping (say, intercept/resend) of any branch of the quantum channel can be detected since the eavesdropper randomly chooses bases in an attack and hence some information must be randomized, which leads to the possibility that the legitimate users disagree. The multi-user situation provides more opportunities for eavesdroppers, the case will hence be more complicated. For the fun-shaped configuration, F_1, an eavesdropping attack can be detected only by the pair of users (including the chair) whose communication have been attacked. For the series configuration, S_1, a single eavesdropping will affect later communications for the rest of users. Once an attack has been detected, the key establishment has to be restarted after all eavesdroppers have been removed. A eavesdropper can only avoid being detected, if she manages to choose the correct measuring basis as targeted legitimate users. This is not possible unless she gets access to at least one of the random number generators used by the legitimate users.

For configurations F_2 and S_2, before sending the conference key distribution, U_0 must make sure whether all private keys are secure. To do this, user U_i sends U_0 a string message encrypted by the private key distribution $k_{U_0U_i}$, through a classical channel. After U_0 has decrypted it also using $k_{U_0U_i}$ she had, U_i speaks publicly about the content of the message. If U_0 finds the message she has measured is not identical to that of U_i, she can then aware that the private key is not secure and remove the eavesdropper afterward. The same procedure should go through all users.

All conference key distribution protocols in this paper are based on BB protocol. In order to be more convenient for our analysis in the rest of the paper, we define two conditions:

Condition ζ_1: U_0 sends U_i a random sequential photon pulses based on four canonical kinds of photon states related to bases B_1 or B_2. We assume that the chance for each state is equal. Consistently, there also is an equal probability for "0" and "1". U_i measures it choosing measuring operator $\hat{O}_{B_1}$ or $\hat{O}_{B_2}$ randomly and independently, so that the chance for each operator is also equal, 50/50. However, they *do not* carry out any public discussion which measuring basis (operator) has been used. Please note that if the basis used by U_i is wrong, U_i has 50/50 of chance to obtain "0" and "1".

Condition ζ_2: Initially, same as condition ζ_1. But they then discuss publicly which

basis is correct in each measurement and agree to discard all photon pulses that incorrect bases have been used by U_i in the measurement.

In the following study, we assume that all eavesdroppers use the way of "intercept/resend" and the measuring approach like that of legitimate user U_i, i.e. randomly choosing measuring basis by a 50/50 of chance.

3 Information Theory of MultiUser Cryptosystems

3.1 Mutual Information in Quantum Channels

We now develop the information formalism for the multiuser system of quantum cryptography, based on the information theory [10] and the work by Barnett and Phoenix [11].

We first consider a two-user quantum cryptosystem based on BB protocol. Assuming that there are two users, A and B, the average mutual information can be defined:

$$I(\hat{B},\hat{A}) = H(\hat{B}) - H(\hat{B}|\hat{A}), \tag{8}$$

where

$$\begin{aligned} H(\hat{B}) &= -\sum_{i=1}^{2} P(b_i)\log_2 P(b_i), \\ H(\hat{B}|\hat{A}) &= -\sum_{i=1}^{2}\sum_{j=1}^{2} P(a_i)P(b_j|a_i)\log_2 P(b_j|a_i), \end{aligned}$$

where the lower-case characters represent eigenvalues of corresponding operator. $\hat{A}$ ($\hat{B}$) is a quantum-mechanical operator denoting a measurement by A (B). $\hat{A}$, $\hat{B} \in \{\hat{O}_{B_1}, \hat{O}_{B_2}\}$. Using quantum-mechanical states to represent the condition probabilities, we have $P(b_j|a_i) \equiv |\langle a_i|b_j\rangle|^2$.

Under BB protocol, Eq. (8) becomes

$$I(\hat{B},\hat{A}) = 1 + \frac{1}{2}\sum_{i=1}^{2}\sum_{j=1}^{2} P(b_j|a_i)\log_2 P(b_j|a_i), \quad \text{(bits)}. \tag{9}$$

This quantity varies between 0 and 1. The information for condition ζ_1 can be obtained:

$$I(\hat{B},\hat{A}) = \frac{3}{4}\log_2 3 - 1. \tag{10}$$

In the presence of Eve, the information is unavoidably affected. The probability is then given by

$$I_E(\hat{B},\hat{A}) = 1 + \frac{1}{2}\sum_{i=1}^{2}\sum_{j=1}^{2}[\sum_{k=1}^{2} p(b_j|\epsilon_k)p(\epsilon_k|a_i)]\log_2[\sum_{k=1}^{2} p(b_j|\epsilon_k)p(\epsilon_k|a_i)]. \tag{11}$$

Under condition ζ_1 we obtain the mutual information when Eve is present,

$$I_E(\hat{B},\hat{A}) = \frac{1}{8}(3\log_2 3 + 5\log_2 5) - 2. \tag{12}$$

Following Barnett et al. [11], we introduce a dimensionless parameter ξ_{AB} defined by

$$\xi_{AB} = \frac{I_E(\hat{B},\hat{A}) - I(\hat{B},\hat{A})}{I_{max}(\hat{B},\hat{A})}, \tag{13}$$

where the maximum mutual information I_{max} is 1 in above cases and $-1 \leq \xi_{AB} \leq 1$. $\xi_{AB} < 0$ indicates the eavesdropper has causes a reduction of information in the quantum channel between A and B and $\xi_{AB} > 0$ indicates an increase of information. $\xi_{AB} = 0$ represents the absence of eavesdropping, or say the eavesdropping is undetectable which occurs only to the case of the eavesdropper having chosen identical measuring bases as B. Fortunately, the chance is almost null when the size of the information string is large. Using Eqs. (10) and (12) we obtain: $\xi_{AB} = -0.1431$, the evidence of eavesdropping.

For condition ζ_2, in the absence of eavesdropping, from Eq. (9) we obtain the mutual information $I(\hat{B},\hat{A}) = 1$ if the measurement via B is prefect; in the presence of eavesdropping, the mutual information is $I_E(\hat{B},\hat{A}) = \frac{3}{4}\log_2 3 - 1$. Using Eq. (13), we obtain $\xi_{AB} = -0.8$, also showing a signature of eavesdropping.

Next, we consider conference key distribution systems. For type F_1, we assume that the discrete quantum channels can be treated to be an integrated channel, which is valid if U_0 sends an identical photon signal to all other users. In a general case, the presence of N_E eavesdroppers, If each invaded quantum channel has only an invader who attacks only once, using condition ζ_2 the mutual information can be expressed as

$$I_{F_1} = I(\hat{X},\hat{U}_0) = W + \frac{1}{2}\sum_{i=0}^{1}\sum_{j=1}^{2^W} P(x_j|u_0 = i)\log_2 P(x_j|u_0 = i), \tag{14}$$

where $\hat{X} = (\hat{U}_1, \hat{U}_2, \cdots, \hat{U}_{N-1})$; accordingly, the eigenvalues $x = (u_1, u_2, \cdots, u_{N-1})$, where $u_j =$ "0" or "1"; x_j denotes the jth state of x and

$$W = \begin{cases} N_E + 1, & \text{if } N - N_E > 1 \text{ and } N_E > 0 \\ N_E, & \text{if } N - N_E = 1 \text{ and } N_E > 0 \\ 1 & \text{if } N_E = 0 \end{cases}$$

and

$$\begin{aligned} P(x_j|u_0 = i) &= P(u_1, u_2, ..., u_{N-1}|u_0 = i) \\ &= P(u_1|u_0 = i)P(u_2|u_0 = i)\cdots P(u_{N-1}|u_0 = i), \end{aligned} \tag{15}$$

which is the conditional probability including N_E eavesdropping attacks. For example, if there are four users, i.e. $\hat{X} = (\hat{U}_1, \hat{U}_2, \hat{U}_3)$ and we assume that the eavesdropper only appears between the quantum channel U_0U_1, x has four states: $x_1 = (0,0,0)$; $x_2 = (1,0,0)$; $x_3 = (0,1,1)$; $x_4 = (1,1,1)$, then we can use Eq. (15) to calculate the conditional probability, for instance

$$\begin{aligned} P(x_1|u_0 = 0) &= P(u_1 = 0, u_2 = 0, u_3 = 0|u_0 = 0) \\ &= P(u_1 = 0|u_0 = 0)P(u_2 = 0|u_0 = 0)P(u_3 = 0|u_0 = 0) \\ &= 3/4 \times 1 \times 1 = 3/4, \end{aligned}$$

and so on. Our discussion is valid only if the following assumption is true, when a user chooses a wrong basis he has a 50/50 chance of receiving "0" and "1", which is consistent with condition ζ_2. When it is eavesdropper free, Eq. (14) gives: $I_{F_1} = 1$.

The information loss due to eavesdropping is an increasing function as the number of eavesdropper. Consistently, the mutual information expressed by Eq. (14) is an decreasing function of the number of eavesdropper. As an example, we calculate the information of four legitimate users as a function of N_E,

$$\begin{aligned} N_E = 1, \quad I_{F_1} &= 0.824; \\ N_E = 2, \quad I_{F_1} &= 0.648; \\ N_E = 3, \quad I_{F_1} &= 0.0715. \end{aligned}$$

The result presented here is obtained by using condition ζ_2 and assuming the eavesdroppers do not add in any their own information.

For type S_1, the series configuration, a signal pulse has to be measured and resent (if it is correctly measured) by each user, one after the other. In order to study the mutual information for the system, we first introduce a transition probability matrix between legitimate users U and V, under condition ζ_2,

$$Q_{UV} = \begin{pmatrix} q_{u_0v_0}, & q_{u_0v_1} \\ q_{u_1v_0}, & q_{u_1v_1} \end{pmatrix}, \tag{16}$$

where

$$q_{u_iv_j} = P(v = j|u = i).$$

The subscripts 0 and 1 denote the binary signal.

The transition probability matrix for users U_0 and U_i in the series configuration then is

$$Q_{U_0U_i} = Q_{U_0U_1}Q_{U_1U_2}Q_{U_2U_3}...Q_{U_{i-1}U_i}. \tag{17}$$

The joint probability is, in terms of the transition matrix, given by

$$P(u_i = j, u_0 = k) = P(u_0 = k) q_{u_{0,k} u_{i,j}}, \qquad (k, j = 0, 1). \tag{18}$$

The mutual information for quantum channel between U_0 and U_i is defined by

$$I(\hat{U}_i, \hat{U}_0) = 1 + \frac{1}{2} \sum_{k,j=0}^{1} P(u_i = j | u_0 = k) \log_2 P(u_i = j | u_0 = k). \tag{19}$$

Assume that there are N users and N_E eavesdroppers ($N - 1 \geq N_E \geq 0$) and each one quantum channel connecting two neighboring users has at most one eavesdropper. So N_E quantum channels are attacked. For simplicity, we further assume that the first N_E quantum channels are targeted. The transition probability matrix can then be expressed to be

$$Q_{u_0, u_{N-1}} = Q_1^{N_E} Q_2^{N - N_E - 1}, \tag{20}$$

where Q_1 is the transition probability matrix between two neighboring users whose channel is attacked and Q_2 is an ordinary transition probability matrix of two attack-free neighboring users. After a simple calculation, we find

$$Q_1 = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}, \qquad Q_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{21}$$

where we have used the condition ζ_2. In terms of Eqs. (18) and (16), we find the average mutual information

$$I_{S_1} = \begin{cases} 1, & (N_E = 0) \\ \frac{1}{N-1} [\sum_{k=1}^{N_E} I(\hat{U}_0, \hat{U}_k) + (N - N_E - 1) I(\hat{U}_0, \hat{U}_E)], & (N_E \geq 1) \end{cases} \tag{22}$$

where

$$I(\hat{U}_0, \hat{U}_k) = \begin{cases} 1 - \frac{3}{4}(k+1) + \frac{1}{2^{k+1}} \log_2 [(2^k - 1)^{(2^k - 1)} (2^k + 1)^{(2^k + 1)/2}], & (k \leq N_E) \\ 1, & (N_E = 0) \\ I(\hat{U}_0, \hat{U}_{N_E}). & (k > N_E \geq 1) \end{cases} \tag{23}$$

Similar to the case of type F_1, I_{S_1} is also an decreasing function of the number of eavesdropper.

In condition ζ_2, we have mentioned that a photon pulse which has been measured using a wrong basis is discarded, so only those photon pulses correctly measured are considered in the calculation of Eqs. (14) and (22). However if we consider all information sent by U_0 including those discarded afterward, the general mutual information should have a factor

of $1/2^{N-1}$ because in fact only $1/2^{N-1}$ of total photon pulses contribute to the conference key distribution. This implies that the mutual information is a decreasing function of the number of user N.

3.2 Mutual Information of Combined Channels

For type F_2, a private quantum key distribution for each quantum channel is established after the chair U_0 has chosen a conference key distribution. A zero information string containing the Boolean addition of both related private key and the conference key is respectively sent to other legitimate users through classical channels by the chair. Obviously, The total information involves both quantum and classical channels. Assuming that the conference key distribution generated by U_0 is one of $K_{U_{0,1}}, K_{U_{0,2}}, ...K_{U_{0,m}}$, where m is total permutations for a certain size of string. The conference key distribution received by another user U_i might not be the original one due to the possibility of break-in of eavesdroppers in the quantum channels, thus we assume it to be one of $K_{U_{i,1}}, K_{U_{i,2}}, ...K_{U_{i,m}}$. Accordingly, the private quantum key distribution obtained by U_0 is one of $k_{U_{0,1}}, k_{U_{0,2}}, ...k_{U_{0,m}}$; the private quantum key distribution of U_i is one of $k_{U_{i,1}}, k_{U_{i,2}}, ...k_{U_{i,m}}$, where each key distribution has the same size as that of the conference key distribution. The mutual information of a pair of users $U_{0,s}$ and $U_{i,t}$, for a general case including eavesdropping is given by

$$I(K_{U_i}, K_{U_0}) = \log_2 m + \frac{1}{m} \sum_{s,t=1}^{m} P(K_{U_{i,t}}|K_{U_{0,s}}) \log_2 P(K_{U_{i,t}}|K_{U_{0,s}}), \tag{24}$$

where the conditional probability of $K_{U_{i,t}}$ given $K_{U_{0,s}}$ is

$$\begin{aligned} P(K_{U_{i,t}}|K_{U_{0,s}}) &= \frac{1}{P(K_{U_{0,s}})} \sum_{l=1}^{m} P(K_{U_{i,t}}, K_{U_{0,s}}, K_{U_{0,l}}) \\ &= \frac{1}{P(K_{U_{0,s}})} \sum_{l=1}^{m} P(k_{U_{i,t'(s,t,l)}}, K_{U_{0,s}}, k_{U_{0,l}}) \\ &= \sum_{l=1}^{m} P(k_{U_{i,t'(s,t,l)}}|k_{U_{0,l}}, K_{U_{0,s}}) P(k_{U_{0,l}}), \end{aligned} \tag{25}$$

where $k_{U_{i,t'(s,t,l)}} = K_i \oplus k_l \oplus K'_j$ and $t'(s,t,l)$ is a function of s, t, and l. If all eavesdroppers are absent and all measurement is prefect,

$$P(K_{U_{j,t}}|K_{U_{i,s}}) = \begin{cases} 1 & (s = t, \text{for all } i, j,) \\ 0 & (s \neq t) \end{cases} \tag{26}$$

Eq. (24) can been used to calculate average mutual information for configurations F_2 and S_2,

$$I_{F_2} = \frac{1}{N-1} \sum_{i=1}^{N-1} I(K_{U_i}, K_{U_0}). \tag{27}$$

However, for the series configuration, type S_2, the conference key transition probability matrix between U_0 and U_i must be given. For any two users, say U_i and U_j, the transition matrix is

$$Q_{U_i,U_j} = \left(P(K_{U_{j,t}}|K_{U_{i,s}})\right)_{m\times m}, \tag{28}$$

where $s,t = 1,2,3,\cdots,m$. Thus the conference key transition probability matrix between U_0 and U_i is expressed as

$$Q_{U_0,U_i} = Q_{U_0,U_1} Q_{U_1,U_2} ... Q_{U_{i-1},U_i}. \tag{29}$$

Eq. (24) can also be used to the mutual information for type S_2.

A advantage of systems of F_2 and S_2 is that the information does not a decreasing function of the number of user N, but types F_1 and S_1 do. This is because, for F_2 and S_2, the quantum key distribution is established between each pair of users, i.e. $N = 2$, but not among all users.

Considering eavesdropping, the average mutual information for types F_2 can be written as:

$$I_{F_2} = \frac{1}{N-1}[(N - N_E - 1)\log_2 m + \sum_{l=1}^{N_E} I_{U_0U_l}] \tag{30}$$

and

$$I_{S_2} = \frac{1}{N-1}[(N - N_E - 1) I_{U_0U_{N_E}} + \sum_{l=1}^{N_E} I_{U_0U_l}] \tag{31}$$

respectively. In Eq.(31) we have assumed the first N_E channels are attacked. It can be shown that $I_{F_2} > I_{S_2}$, if $N - 1 \geq N_E > 0$.

4 Correlations in Quantum Cryptosystems

4.1 Correlation in Quantum Channels

The information theory can describe increase/decrease of information in quantum conference cryptosystems due to eavesdropping, as studied above. However, we find that in some circumstance, the system mutual information is not completely reliable for a small size of signal string. As an example, see Fig. 2, A sends "0" or "1" to B who then obtains

"0" or "1" with probability of either 0 or 1. There are two completely different cases: in Fig. 2(a), B receives totally wrong signal; in Fig. 2(b), B receives the correct signal. It is easy to find that the mutual information for both cases has the same value, $I(\hat{B}, \hat{A}) = 1$. We therefore consider another way to estimate the merit of cryptosystem: by means of correlation between users.

For two users, A and B, the correlation function of A and B is defined by

$$C(\hat{A}, \hat{B}) = \frac{cov(X_{\hat{A}}, X_{\hat{B}})}{[var(X_{\hat{A}})var(X_{\hat{B}})]^{1/2}}, \tag{32}$$

where random variables $X_{\hat{A}}$ and $X_{\hat{B}}$ are 0 when "0" is measured and 1 when "1" is measured. $\hat{A}$ is a measuring operator used by A and $\hat{B}$ is the measuring operator used by B. If the communication is prefect, $C(\hat{A}, \hat{B}) = 1$, A and B are then said to be perfectly correlated. If $C(\hat{A}, \hat{B}) = 0$, A and B are uncorrelated. When A and B are independent, i.e. the communication completely fails, $C(\hat{A}, \hat{B}) = 0$. Therefore the case that communication completely fails belongs to $C(\hat{A}, \hat{B}) = 0$. Between 0 and 1 is partially correlated. If the sent and received signals are negatively-correlated, $C(\hat{A}, \hat{B}) = -1$. For the cases illustrated in Fig. 2, $C(\hat{A}, \hat{B}) = 1$ and -1 respectively.

If there is no any invader between A and B, whether B receives a correct message depends only on whether B uses a correct basis as A does. We assume that the eigenvalues of $|\rightarrow\rangle$ and $|\uparrow\rangle$ are "0" respectively; the eigenvalues of $|\leftarrow\rangle$ and $|\downarrow\rangle$ are "1" respectively. It is easy to obtain: under condition ζ_1, $C(\hat{A}, \hat{B}|\zeta_1) = 1/2$.

Under the condition ζ_2, if the measurement of B is 100% correct, it is easy to find $C(\hat{A}, \hat{B}|\zeta_2) = 1$. If there is an invader E who is eavesdropping between A and B, for the former case above, $C(\hat{A}, \hat{B}|\zeta_1) = 1/4$; for the later case, $C(\hat{A}, \hat{B}|\zeta_2) = 1/2$. These values suggest that the eavesdropping has decreased the correlation.

Next, we consider multiuser cases. Assuming that U_0 is the chair of a conference, who takes charge of the conference key communication. The average correlation for N users is

$$\bar{C} = \frac{1}{N-1} \sum_{i=1}^{N-1} \frac{cor(X_{\hat{U}_0}, X_{\hat{U}_i})}{[var(X_{\hat{U}_0})var(X_{\hat{U}_i})]^{1/2}}, \tag{33}$$

where $\hat{U}_i$ denotes an operator by another user U_i. The formula can be applied to both type F_1 and S_1. It is easy to show that when eavesdropping is absent, $\bar{C}$ has the same value as in the two-user case.

When eavesdropping is present, for type F_1, assuming that each branch of quantum channel has at most one eavesdropper, we have

$$\bar{C} = 1 - \frac{N_E}{2(N-1)}. \tag{34}$$

N_E is the number of eavesdroppers. It is found that $\bar{C} \in \{0.5, 1\}$. Here we have used the condition ζ_2.

For type S_1, the series configuration, we have introduced a transition probability matrix, Eq. (17) and obtain the joint probability, Eq. (18). The average correlation can be obtained in terms of the transition probability matrix, using Eq. (33).

If there are N users and N_E eavesdroppers who attack the quantum channels of the first N_E pairs of users, using Eq. (21) and condition ζ_2 we obtain the average correlation for type S_1

$$\bar{C} = \frac{1}{N-1}[\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^{N_E}} + (N - N_E - 1)\frac{1}{2^{N_E}}], \quad (N_E > 0). \tag{35}$$

If the invader attacks the quantum channel between U_0 and U_1 only, $\bar{C} = 1/2$.

4.2 Correlation in Combined Channels

Similar to the case of information studied in Section 3, For both configurations F_2 and S_2, private keys have to be established between each pair of users through quantum channels for late sending the conference key distribution chosen by U_0. The correlation between sent and received conference key distribution is given in this section.

We first define a transition matrix between U_i and U_j,

$$Q(U_i, U_j) = \left(P(K_{U_{j,t}}|K_{U_{i,s}})\right)_{m\times m}. \tag{36}$$

The joint probability of U_i and U_j is

$$P(K_{U_{j,t}}, K_{U_{i,s}}) = P(K_{U_{i,s}})P(K_{U_{j,t}}|K_{U_{i,s}}). \tag{37}$$

Note that $\{K_{U_{i,t}}\}$ has m states and $K_{U_{i,t}}$ and $K_{U_{j,t}}$ represents the same conference key distribution for any i and j, $t = 1, 2, ..., m$.

In order to calculate correlation between sent and received conference key distribution, we introduce two random variables, X_{U_i} and X_{U_j}, taking values

$$X_{U_0} = s, \quad \text{if } K_{U_{0,s}} \text{ is sent,}$$
$$X_{U_i} = s, \quad \text{if } K_{U_{i,s}} \text{ is received,}$$

where $s = 1, 2, ..., m$.

Hence the correlation between information received by U_0 and U_i can be obtained in terms of the formula:

$$C(X_{U_0}, X_{U_i}) = \frac{cov(X_{U_0}, X_{U_i})}{[var(X_{U_0})var(X_{U_i})]^{1/2}}. \tag{38}$$

The system correlation is defined as the average correlation over all users, being the same as Eq. (33).

5 Discussion and Conclusion

More general quantum conference key distribution systems can be established in terms of the basic structures studied in previous sections. The most straightforward model is ring-configuration, as shown in Fig. 3(a), which can be referred to the series configurations. In Fig. 3(b), a configuration based on a combination of series configurations is shown. Each branch can be treated as a group that has been discussed in previous sections. The final conference key communication can be carried out utilizing the boolean addition and a classical channel. Fig. 3(c) exhibits a tree configuration, which is based on either J_{B_1} or J_{B_2}.

The number of user in each group seems important for types F_1 and S_1, since as mentioned previously, the mutual information is a decreasing function of N. In order to increase the information rate in a large the number of user, U_0 has to increase the size of information string, which, we believe, will cost communication time. A reasonable N should be chosen according to physical requirement for a practical system.

The conference key distribution is sent to each group by the chair using classical channels and Boolean addition. In the absence of eavesdropping, each group can have a perfect group key distribution. The correlation and information for the channels between groups can be calculated in terms of the method introduced in the previous sections, provided we treat a group as a user. However, in the presence of eavesdropping, some group key distributions might have been badly hurt, hence the calculation becomes complicated. Under such situation, the calculation has to rely on users' keys and relevant quantum channels because the case is different from user to user. The security of a conference key distribution is based on each group key distribution, where since the establishment of group key distributions involves quantum channels, any attack(s) can be detected before the final conference key distribution is sent by the chair. Consequently, a secure conference key distribution can be established, after all eavesdroppers are removed.

In conclusion, in this paper we have developed quantum conference key distribution system based on four basic protocols. The mutual information and correlation between users have been studied for the cases that eavesdropping is present. The security in these systems is based on cryptographic communication in each quantum channel, where any

eavesdropping can be detected. Therefore our systems are secure against intercept/resend attacks. On the other hand, we show that types F_1 and S_1 have the disadvantage in the restriction of user's population. Also the other disadvantage which should be pointed out here is that two attacks on such systems is enough to extract all information, if the attackers measure two separated quantum channels using two different measuring operators, for example $\hat{O}_1$ for channel one and $\hat{O}_2$ for channel two. Fortunately, as mentioned before, any such an attack can be detected by relevant users, since some data must be randomized during the attack. The configurations of F_2 and S_2 are more secure comparing with types F_1 and S_1. This is because each pair of legitimate users use the different quantum protocol to transmit signal, thus the information extracted by each eavesdropper becomes independent. Many other more complicated quantum conference key distribution systems can be built by utilizing the our four basic protocols. The security in such systems relies on the security of each group key distribution.

ACKNOWLEDGES

The first and second authors were supported in part by the Australian Research Council under the reference number A49232172.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, (Bangalore, India) (1984) pg. 175–179.

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5 (1992) pg. 3–28.

[3] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6 (1991) pg. 661–663.

[4] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, "Practical quantum cryptogaraphy based on two-photon interferometry," *Phys. Rev. Lett.*, vol. 69, no. 9 (1992) pg. 1293–1295.

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5 (1992) pg. 557–559.

[6] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Sinle photon interference in 10 km long optical fibre interferometer," *Electronics Letters*, vol. 29 (1993) pg. 634–635.

[7] Y. Mu, Y. Zheng, J. Seberry, and Y.-X. Lin, "A quantum cryptosystem secure against beamsplitting attcks." (unpublished).

[8] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distributiob system," *IEEE Transcations on Information Theory*, vol. IT-28, no. 5 (1982) pg. 714–720.

[9] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Advances in Cryptography: Proceedings of Crypto '84*, Springer-Verlag, New York, (1984) pg. 475–480,

[10] F. T. S. Yu, *"Optics and Information Theory"*. John Wiley & Sons, New York (1976).

[11] S. M. Barnett and S. J. D. Phoenix, "Information-theoretic limits to quantum cryptography," *Phys. Rev. A*, vol. 48, no. 1 (1993) pg. R5–R9.

Figure Captions:

Fig. 1 The schematic diagram of the quantum conference key distribution cryptosystems with N legitimate users. (a) shows a fun-shaped configuration; (b) shows a series configuration.

Fig. 2 A communication between A and B using only two photon pulses "0" and "1". (a) shows that B has a probability of zero to receive the correct signal and a probability of one to receive incorrect signal. (b) shows that B has a probability of one to obtain the correct signal and a probability of zero to receive incorrect signal.

Fig. 3 Quantum conference key systems based on the fun-shaped and series configuration. The black-solid circle in each diagram represents the chair.